JPRS トピックス＆コラム

■DNSの安全性・安定性向上のためのキホン ～お使いのDNSサーバーは大丈夫ですか？～

DNSサーバーの安全性と安定性を高めるには、それぞれのサーバーの機能や特性に応じた適切な管理運用が必要です。あなたがお使いのDNSサーバーを再確認してみましょう。

■2 種類の「DNS サーバー」に注意

DNS サーバーには、**権威 DNS サーバー**と**キャッシュ DNS サーバー**の 2 種類があります。

権威 DNS サーバーは権威サーバーや DNS コンテンツサーバーなどとも呼ばれ、ドメイン名の階層構造を構成し、名前情報を管理します。それに対し、キャッシュ DNS サーバーはキャッシュサーバーや DNS リゾルバーなどとも呼ばれ、ユーザー（クライアント）の要求を受け権威 DNS サーバー群によるドメイン名の階層構造をたどり、名前解決サービスを提供します（図 1）。

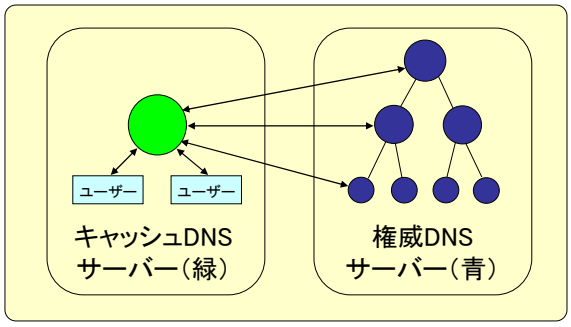

図 1: 権威 DNS サーバーとキャッシュ DNS サーバー

▼権威/キャッシュ DNS サーバーの分離

このように、権威 DNS サーバーとキャッシュ DNS サーバーは本来別の機能を担当しており、サービス対象やその提供範囲も異なっています（表 1）。

	権威 DNSサーバー	キャッシュ DNSサーバー
機能	階層構造を構成し 名前情報を管理する	階層構造をたどり 名前解決を提供する
サービス対象	インターネット上の キャッシュ DNSサーバー	ISPや組織などの ユーザー （クライアント）
サービス提供範囲	インターネット 全体	対象ユーザー （クライアント）のみ

表 1: 機能・サービス対象・サービス提供範囲の違い

DNS サーバーの代表的な実装の一つとして長年利用されている BIND では、権威 DNS サーバーとキャッシュ DNS サーバーの機能を一つのサーバーで兼用することができます。しかし、兼用による影響やセキュリティ上のリスク[1]などを考慮した場合、双方を共有することは好ましくなく、現在では開発元の ISC においても双方を別のサーバーに分離することを推奨しています[2]。

また、DNS Amp 攻撃[3]や DNS キャッシュポイズニング[4]のリスクを軽減する観点からも、**権威/キャッシュ DNS サーバーの分離が強く推奨**されています。

▼分離の際は権威 DNS サーバーの変更がお奨め

多数のユーザー（クライアント）に一度公開したキャッシュ DNS サーバーの IP アドレス変更は、ユーザー側での追加作業や予期しないトラブル発生のリスクを伴います。これに対し、ルートサーバー以外の権威 DNS サーバーの IP アドレス変更では、自身が管理するゾーン情報と上位ゾーン（レジストリなど）の登録情報のみを変更すればよく、キャッシュ DNS サーバーに比べ、変更は比較的容易であるといえます。

そのため、権威 DNS サーバーとキャッシュ DNS サーバーの分離を図る場合、DNS サーバーを新たに準備し[5]、**権威 DNS サーバーの機能のみを新しいサーバーに分離する方法で実施する**のがよいでしょう（図 2）。

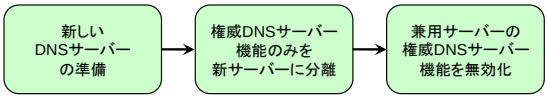

図 2: 権威 DNS サーバーの分離手順

[1]機能の分離により、一方の機能に不具合や脆弱性が発見された場合にも、その影響を回避可能です。
[2]ISC Technical Note: Running An Authoritative-Only BIND Nameserver <http://ftp.isc.org/isc/pubs/tn/isc-tn-2002-2.html>
[3]「JPRS トピックス＆コラム」No.3 を参照。
[4]「JPRS トピックス＆コラム」No.9、No.13 を参照。
[5]必ずしも物理的に別のサーバーにする必要はなく、例えば 1 台のサーバー上に複数の IP アドレスを設定する形で分離する方式も可能です。

※掲載内容は2012年1月現在のものです。

■DNS サーバーの安全性・安定性を高める

権威 DNS サーバーとキャッシュ DNS サーバーを分離することでそれぞれのサーバーに応じた適切な設定が可能になり、DNS サーバーの安全性・安定性を高めることができます。以下、分離後の権威 DNS サーバーとキャッシュ DNS サーバーそれぞれにおいて、特に注意すべきポイントを解説します。

■権威 DNS サーバーにおけるポイント

▼再帰検索要求の受け付けを無効化

権威 DNS サーバーではキャッシュ DNS サーバーの機能を提供する必要がありません。そのため、キャッシュ DNS サーバーでのみ必要となる、再帰検索要求の受け付けを無効に設定しておきます（図 3）。

```
options {
        // アクセスコントロールは実施しない
        //  （インターネット全体にサービスを提供）
        allow-query { any; };
        // 再帰検索要求の受け付けを無効に設定
        recursion no;
};
```

図 3: BIND 9 における設定例

これにより、キャッシュ DNS サーバー機能に脆弱性が発見された場合でも、その影響を回避することが可能になります。また、後述するキャッシュ DNS サーバー機能に存在するセキュリティ上のリスクを回避できます。

■キャッシュ DNS サーバーにおけるポイント

▼適切なアクセスコントロールの実施

通常、キャッシュ DNS サーバーではサービス対象となるユーザー（クライアント）からのアクセスのみを許可すればよく、インターネット全体にサービスを公開する必要はありません。そのため、サービス対象以外からの利用を制限するアクセスコントロールを実施することで、外部からの不正使用を防止できます（図 4）。

```
// 組織内ネットワーク一覧をACLで定義
acl MYNET {
        192.0.2.0/24;
        2001:db8:2::/64;
};
options {
        // 内部からの問い合わせのみ受け付ける
        allow-query { MYNET; };
        allow-recursion { MYNET; };
        allow-query-cache { MYNET; };
};
```

図 4: BIND 9 における設定例

アクセスコントロールは、DNS Amp 攻撃の踏み台となるリスクや、DNS キャッシュポイズニングのリスクを軽減するのにも役立ちます。他の組織やユーザーに迷惑をかけないようにするためにも、キャッシュ DNS サーバーにおけるアクセスコントロールは重要です。

▼ポート番号のランダム化は必須事項

2008 年に発表されたカミンスキー型攻撃手法により、未対策のキャッシュ DNS サーバーに対し数秒以内に DNS キャッシュポイズニングを成功させることが可能になり、攻撃に対するリスクが急速に高まりました。

このため、緊急対策[6]としてキャッシュ DNS サーバーの DNS 問い合わせ用ポート番号をランダム化し、外部からの予測を困難にする対策が実施されました（図 5）。

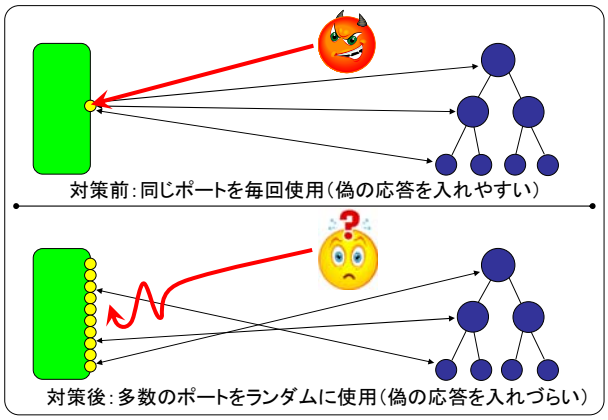

図 5:ポート番号のランダム化による効果

ポート番号のランダム化に対応していないキャッシュ DNS サーバーを使い続けることは**極めて危険**であり、**早急に対応版に切り替える必要があります**。また、キャッシュ DNS サーバーの設定内容や途中のネットワーク機器の仕様などにより、ランダム化に対応した実装であってもポート番号を外部から推測可能な状態になってしまう場合があるため、注意が必要です。

■より詳細な解説を『実践 DNS』に掲載

本コラムで取り上げた内容を含む、DNS サーバーの安全性・安定性を高めるための設定・運用方法に関する解説を、JPRS 監修による書籍『実践 DNS』にまとめています。併せてご利用ください。

[6]より根本的な対策として、DNSSEC の導入が進められています。

